O noua alerta CERT-RO: Conturi de WhatsApp din România,deturnate de catre atacatori prin metode de inginerie sociala

Echipa Centrului National de Raspuns la Incidente de Securitate Cibernetica (CERT-RO) atrage atentia asupra unui tip de atac, care a început sa fie notificat ca incident de catre utilizatori din România, fiind vorba despre încercari ale atacatorilor de a obtine acces la conturile de WhatsApp ale anumitor utilizatori - tinta, prin tehnici de inginerie sociala.

Conform unei notificari postate pe propria pagina de Internet, conturile de WhatsApp sunt legate de numerele de telefon ale utilizatorilor, iar în momentul autentificarii (login) într-un cont existent, aplicatia va trimite automat utilizatorului un "one-time code" (parola unica), prin SMS, pentru a verifica numarul de telefon. În acest sens, atacatorii abuzeaza de acest proces, pentru a încerca preluarea controlului acelor conturi de WhatsApp ale utilizatorilor vizati.

"Atacatorii joaca rolul unui prieten sau a WhatsApp Support Team. În multe cazuri, atacatorii obtin numarul de telefon al unei victime prin intermediul unui cont de WhatsApp deja compromis. Urmatorul pas consta într-o noua instalare a aplicatiei pe telefonul atacatorului, în cadrul careia este furnizat numarul de telefon al victimei. Aceasta va primi prin SMS un cod de înregistrare, care este solicitat ulterior de atacatorul care joaca rolul unui prieten, ori chiar a WhatsApp Support Team", sustin reprezentantii CERT-RO.

De asemenea, infractorii cibernetici folosesc conturi de WhatsApp deturnate pentru a distribui, catre utilizatorii vizati, mesaje ce contin informatii false cu privire la promotii pentru platformele de e-commerce (de exemplu oferte speciale). Prin aceste mesaje, victimele sunt pacalite sa trimita "codul promotional" primit pe telefon, fiind de fapt codul de înregistrare la WhatsApp.

"În situatia în care un utilizator are telefonul închis (de obicei pe timpul noptii), atacatorul poate introduce în mod repetat codul gresit de înregistrare la WhatsApp. Astfel, atacatorul va avea optiunea efectuarii verificarii vocale, în cadrul careia WhatsApp va apela telefonul utilizatorului si va transmite codul citit "cu voce tare" într-un mesaj. Desigur, mesajul audio va fi redirectionat catre mesageria vocala a victimei, care poate fi accesata cu usurinta, în situatia în care victima nu a schimbat parola implicita (default)", avertizeaza specialistii.

În cazul în care contul de Whatsapp a fost pierdut, acesta poate fi recuperat astfel: daca ati fost victima unui astfel de atac, puteti sa intrati în contul de WhatsApp prin intermediul numarului de telefon, dupa care veti primi un nou cod de înregistrare, iar atacatorul va fi delogat.

"Pentru cazul în care atacatorul a activat autentificarea în 2 pasi (2FA), poate fi necesar sa asteptati 7 zile pentru a accesa contul, fara verificarea prin doi pasi. Victimele care prefera sa stearga si sa reinstaleze aplicatia vor pierde istoricul conversatiilor, în cazurile în care nu au la dispozitie copii de siguranta (back-up) anteriorare, care sa functioneze", subliniaza expertii CERT-RO.

CERT-RO are o serie de sfaturi pentru securizarea contului de WhatsApp: activarea optiunii "Two-Step Verification" a WhatsApp, ce poate fi gasita în cadrul setarilor pentru aplicatia WhatsApp; schimbarea PIN-ului pentru mesageria vocala (mai multe informatii în acest sens pot fi obtinute prin contactarea furnizorului de telefonie mobila); nu împartasiti cu nimeni codurile de verificare sau "one-time passwords" specifice contului de WhatsApp; nu raspundeti mesajelor venite de la un contact sau de la un strain, prin care sunt solicitate aceste coduri; nu accesati link-uri si nu oferiti date personale în cadrul acestor conversatii; verificati autenticitatea mesajului prin mijloace alternative, precum apelarea contactului (daca mesajul provine de la un contact necunoscut, raportati numarul catre WhatsApp).